HZ BOOKS
华章科技

涉及普通网民的所有网络活动，抵御网络危险构筑安全环境
网络威胁早知道、反病毒软件会操作、网上应用全攻略

身边的网络安全

互联网时代的生活安全攻略

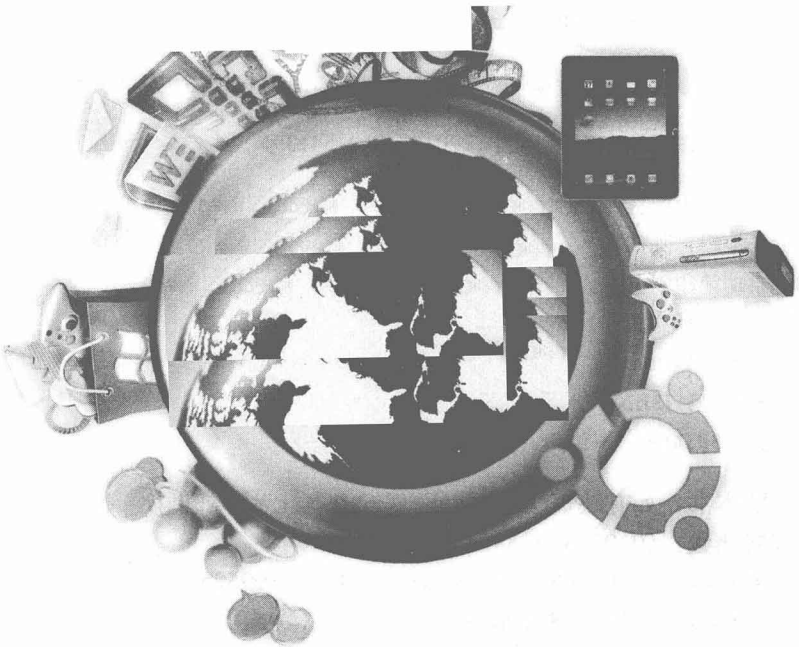
王　杉　李广鹏　史艳艳　编著

机械工业出版社
China Machine Press

身边的网络安全

互联网时代的生活安全攻略

王 杉 李广鹏 史艳翔



机械工业出版社
China Machine Press

本书主要讲述了现代网民身边各式各样的网络威胁以及安全防护常识。首先，以极具说服力的数据展现了危机四伏的现代网络生活。接下来，深入浅出地介绍了人们上网的媒介——电脑平台的运行以及维护常识。然后，将五花八门的病毒以及网络威胁分门别类，针对各自特点进行深入而实用的剖析。最后，分别从网上冲浪、网上聊天、电子邮箱、网络下载、网上交易、网上炒股和手机应用等现代网民的常规网络生活方面，对网络安全的防护原则和方法进行了细致的阐述。

本书内容安排详略得当、覆盖全面，几乎涉及了普通网民的所有网络活动；在各个章节所附加的各种网络威胁的实例及其应对方案也非常实用高效，适合普通网民用来抵御上网危险，营造安全的上网环境。

图书在版编目（CIP）数据

身边的网络安全：互联网时代的生活安全攻略 / 王杉，李广鹏，史艳艳编著. —北京：机械工业出版社，2011.1

ISBN 978-7-111-32420-1

Ⅰ.身… Ⅱ.①王… ②李… ③史… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2010）第215413号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：陈佳媛
北京瑞德印刷有限公司印刷
2011年1月第1版第1次印刷
170mm×242mm · 19印张
标准书号：ISBN 978-7-111-32420-1
定价：39.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

前　言

随着电脑和互联网的普及，越来越多的人参与到了互联网当中。特别是随着3G网络和智能手机的飞速发展，科技已经将网络与现实世界拉得更近。网上冲浪、网上聊天、网络下载、网上交易或者收发邮件，这些网络活动似乎在慢慢地变成人们生活的一部分。互联网的飞速发展实实在在地改变着人们工作、学习和生活的方式。可以说，网络使现代人类生活变得更加轻松。

然而，人们越来越倚重于电脑和网络的时候，却要面临各种各样的网络安全威胁。计算机病毒、网络诈骗、数据丢失和隐私泄露越来越成为网民谈之色变的狠角色。作为没有计算机知识背景的网民朋友，一旦遇到这些威胁，总感觉它们神秘莫测。想要做点事情，却又求助无门。在网络上只能得到一些零星琐碎的知识，翻开教科书又都是针对专业人员的长篇大论，这些对于普通网民有效防范网络威胁都没有太大用处。

针对这种情况，作者决心写一本真正能够帮助普通网民的网络安全书籍，希望将自己多年的网上生活经验分享给广大读者。同时，希望广大网民能够远离网络威胁，尽情享受网络带来的方便与快乐。针对本书的特殊定位，其特点如下：

- 贴近实战。本书大部分篇幅用来介绍在各种上网活动中可能遇到的网络威胁和解决方法。对于主流的病毒或者威胁，都会给出切实可行的解决方法。对于普通用户可能遇到的技术性问题也尽量做了浅显的说明，力图使读者在解决问题的同时，明白其中的基本原理和操作原则。
- 知识全面。本书不但有计算机和互联网相关的基本常识，还将病毒和网络威胁汇总分类。这样做的目的在于将常识背景告诉读者，再结合实际网络活动的实战，潜移默化地培养读者的网络安全意识，最终使读者不但能够应对书中提到的具体实例，还可以举一反三地应对新威胁。
- 操作讲解详尽、清晰。在形式上，所有的操作步骤都配以插图说明，操作步骤非常详细，这样可以使读者更加快速地学习本书中的内容。
- 内容安排详略得当。网络安全往往是一个宽泛的话题，本书则精心挑选了

普通网民最需要的知识进行介绍。对于理论知识只求能够让读者大概了解，着墨不多；而对于网民最需要的网络安全防护方法则详尽介绍。这样安排有利于读者快速解决问题，又不会步入技术上的误区。

- 精确导航，内容精练。所有章节均有本章导航内容，总结了全章所要讲述的主要内容，让读者可以迅速定位到自己感兴趣的章节。

本书共分为10章，具体安排如下：

第1章介绍了丰富多彩的网络生活中的种种威胁，以及它们造成的巨大危害，以此来警戒人们提高网络安全意识。

第2章介绍了电脑程序、互联网的基本运行原理，以及应如何打造一个相对安全的上网平台。

第3章将矛头直指计算机病毒和其他网络威胁，分别对普通病毒、蠕虫、木马和网络钓鱼等进行了细致的剖析和讲解。除了介绍其危害原理和传播途径外，还给出了一些比较有效的防范技巧和方法。

第4章~第9章分别讲述了上网冲浪、即时通讯软件、电子邮件、网络下载、网上购物和网上炒股等活动中经常遇到的网络威胁和防范方法。这些内容已经涵盖了普通网民的所有上网活动，经常遇到安全威胁的读者可以直接查阅这些章节获取相关防护知识。

第10章针对近来不断升温的手机网络安全问题，主要是帮助手机上网用户防护各种威胁。

本书主要由王杉、李广鹏和史艳艳编写，其他参与校对的人员包括张铮、王命达、马宏和杜强等。在本书策划、编写以及校对过程中，得到了金羽图书工作室的大力支持，张铮老师对本书做了大量的修改工作并提出了许多中肯的意见和建议，在此一并表示感谢。

虽然作者力求本书内容臻于完美，但由于水平所限，时间仓促，疏漏之处在所难免，还望广大读者批评指正。如果您在阅读的过程中有任何问题，请登录金羽图书工作室的网站www.book95.com的计算机知识讨论区，或金羽图书先锋答疑QQ群：112812004，在这里将会得到图书作者或者专业人士的详细解答。

目　录

第1章

我们生活的网络时代

如今，网络已经成为我们日常生活中不可或缺的一部分。我们无时无刻不在和网络打交道——查资料、玩游戏、看电影、听音乐、聊天和疑问求助等。可以毫不夸张地说，互联网（Internet，即因特网）的诞生与发展改变了整个人类世界的生活方式。然而，现在的网络在蕴藏着丰富资源的同时，也充斥着木马和病毒，我们稍有不慎就会中招：刚安装的新系统，几天后就开始频繁死机，或是上网速度越来越慢；登录QQ，突然提示密码错误（被盗号）；想浏览网页，却弹出数不尽的窗口；有些病毒竟然还能破坏电脑中的重要文件和盗取私人重要信息，时刻威胁着用户的隐私安全。面对这些，难道绝大多数网民就只能是恐惧和无奈吗？！

本章导航

- ❑ 计算机病毒给人类带来的巨大损失
- ❑ 常见的网络威胁
- ❑ 计算机病毒的发展和分类
- ❑ 防范计算机病毒的原则

1.1 病毒泛滥的信息时代

随着PC（个人计算机）及互联网的普及，计算机病毒也随之泛滥，网络威胁日益升级。据报道，每天都会产生十多种计算机病毒，世界各国遭受计算机病毒感染和攻击的事件数以亿计，严重地干扰着人们的正常生活，给全人类造成了巨大的经济损失和安全威胁。

1.1.1 病毒让世界损失严重

从1982年攻击个人计算机的第一款全球病毒诞生到现在已经有28年的时间，在这期间病毒的种类和破坏方式不断翻新。特别是随着互联网络的发展，病毒带来的损失呈现范围广、数量大的趋势。

2000年，互联网发展方兴未艾。一种叫做“爱虫”（Love bug）的病毒就以极快的速度感染了全球范围内的个人计算机系统，如图1-1所示。这种病毒属于蠕虫类脚本病毒，通过电子邮件附件进行传播，对电子邮件系统产生极大的危害。该病毒在传播的数小时内就感染了大量的个人计算机系统，几乎使得整个网络系统瘫痪。

2001年，当个人计算机迎来它的20岁生日之际，恶毒的“CAM先生”病毒和“红色代码”病毒通过网络袭击了全球的计算机系统，在短短数天的时间里已经让美国损失了近20亿美元，给人类带来巨大损失。同年，美国将近数百万的电脑被“求职信”（Wantjob）病毒攻击导致瘫痪，大量政府机构与企业的网络根本无法运行。如此猖狂的病毒让办公人员闻毒色变，如图1-2所示。

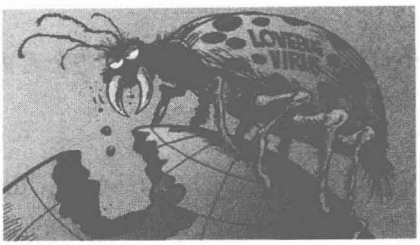


图1-1　全球肆虐的爱虫病毒

图1-2　办公人员工闻毒色变

2003年8月，电脑病毒——“冲击波”突袭，全球混乱，如图1-3所示。人们惊呼，“冲击波”开辟了电脑病毒新的攻击传播方式，是病毒史上“从被动进攻到主动进攻”的突破，引爆了新一轮病毒高峰！该病毒不但本身破坏力巨大，可以使被感染电脑不断重启，而且还可以通过植入其他病毒对电脑造成破坏，如利用“CIH”病毒破坏计算机硬盘等。因此，“冲击波”病毒给人类造成的损失，轻而易举超过了之前的“红色代码”病毒（全球企业和个人经济损失共26.2亿美元）。当时国内的计算机保有量已初具规模，但防范措施和技术都未能跟上，因此该病毒也第一次引起了国内计算机用户对病毒的关注。

图1-3　冲击波病毒在全球传播

“冲击波”还未走远，2004年4月30日“震荡波”（Sasser）病毒就爆发了。这是一个利用微软操作系统的LSASS漏洞通过445连接端口对全球网络发动攻击的蠕虫病毒。该款病毒已经不再需要通过电子邮件来传播，任何开机并且连上互联网的计算机都可能感染它。在短短的十几天内，该病毒即席卷了全世界，造成数千万的电脑瘫痪，数亿财产付之东流。“震荡波”也由于其较大的破坏性，被人们戏称为2004年的“毒王”，如图1-4所示。

图1-4　破坏巨大的震荡波病毒

以上介绍的病毒在破坏性、传染性等方面可谓是独领风骚，但是造成人类损失的病毒远非以上几种。下面简单介绍2004年的几个“毒王”，使大家认识到病毒的厉害之处。其后的病毒更是逐年增加，不胜枚举。

（1）网络天空及变种

2004年2月19日网络天空病毒（I-Worm/NetSky.b）被首次截获后，9个月内，该病毒几乎每天都以最高上报率和最高爆发率蝉联病毒榜榜首。

（2）网银大盗及其变种

“网银大盗”是2004年上半年产生的以专门偷窃资金为目的的木马病毒。由于发现及时，网银大盗并没有造成很大的经济损失，但是其偷窃亿万网上资产的险恶用心可谓歹毒。根据其巨大的潜在危害性，网银大盗位列2004年十大病毒前三甲。

（3）“雏鹰”病毒及其变种

2004年1月19日，“雏鹰”蠕虫病毒首次被截获。有趣的是，在后期的变种中，“雏鹰”病毒作者和“网络天空”病毒作者互相指责对方盗窃了其病毒源代码，在向外传播的时候也不忘骂上几句，甚至变种I-Worm/BBEagle.o如果发现用户计算机已经感染了“网络天空”病毒，会自动将其清除。该病毒造成的损失和“网络天空”相比可谓不分伯仲。

（4）证券大盗

证券大盗是病毒家族中的晚辈，刚出生不久便在2004年11月25日被截获。但是其潜在的巨大危害让人们不得不对其刮目相看。它的主要特征是偷盗的隐蔽性，能够盗窃股票账号操纵交易，直接威胁资产数目之大不亚于“网银大盗”。“证券大盗”之毒，引起了有正义感的黑客团体的愤怒，就在其产生后的一周内，其网页就被黑客黑掉了。

（5）“超级密码杀手”病毒及变种

“超级密码杀手”（也叫“爱情后门”）是个成员众多的病毒族群。它是一种具有木马功能的蠕虫，能够以最隐蔽的手法获得并复制目标数据库的密码。它还能够自动搜索并终止杀毒软件的运行，其潜在危害可见一斑。

（6）PolyBoot引导区病毒

PolyBoot（也叫WYX.B）是一种典型的感染主引导扇区和第一硬盘DOS引导区的内存驻留型和加密引导型病毒。它不会感染和破坏任何文件，但一旦发作，就会使硬盘所有的分区及数据丢失。感染对象可以是任何的平台，包括Windows、Unix、Linux、Macintosh等。

1.1.2 国内反病毒形势严峻

伴随“震荡波”病毒的肆虐，国内的上网安全漏洞集中地暴露出来。之后的几年间，越来越多的病毒呈现本土化趋势，并向地域化发展。各种病毒及其变种伴随着与各个杀毒软件的较量数目在不断增加。由于中国的计算机用户数量增长迅速，且大多数新增用户网络安全意识较差，导致国内地域化的病毒爆发频繁，

破坏性巨大。

一些读者可能还记得2007年红遍全国的“熊猫烧香”病毒，它会使所有程序图标变成“熊猫烧香”，如图1-5所示，并使其不能运行。更可恶的是，该病毒还会删除扩展名为gho的文件，使用户无法使用ghost软件恢复操作系统。

图1-5　“风靡一时”的“熊猫烧香”病毒

“熊猫烧香”感染系统的“.exe”、“.com”、“.f”、“.src”、“.html”和“.asp”文件，添加病毒网址，导致用户一打开这些网页文件，IE浏览器就会自动连接到指定的病毒网址中下载病毒。该病毒在硬盘各个分区下生成文件autorun.inf和setup.exe，可以通过U盘和移动硬盘等方式进行传播，并利用Windows系统的自动播放功能来运行。同时，它会在中毒电脑中所有的网页文件尾部添加病毒代码。一些网站编辑人员的电脑如果被该病毒感染，上传网页到网站后，就会导致用户浏览这些网站时也被病毒感染。据悉，多家著名网站已经遭到此类攻击，而相继被植入病毒。由于这些网站的浏览量非常大，致使“熊猫烧香”病毒的感染范围非常广，中毒企业和政府机构已经超过千家，其中不乏金融、税务和能源等关系到国计民生的重要单位。

进入2008年，全国人民正在喜庆的气氛中迎接奥运会的到来。但就在这一年一种利用系统漏洞从网络入侵的病毒——“扫荡波”开始蔓延。它的快速传播带有一定的讽刺性。当时恰逢微软打击盗版系统的黑屏事件，大批用户关闭了系统的自动更新功能，从而让该病毒有机可乘。该病毒的主要危害在于被攻击者的机器可以完全被控制，如图1-6所示。

图1-6　电脑被控制

当人们还沉浸在新年合家团聚的氛围中时，虎年病毒早已虎视眈眈地瞄准了用户上网比较集中的时段。由金山云安全监测中心于2010年1月4日发布的最新数据显示，2010年元旦3天，互联网新增电脑病毒、木马近50万。其中网页挂马再度出现高发期，仅1月1日一天，全国被挂马网址多达20万。2010年元旦前后的一个月中，不少网络病毒横行，其中包括已感染全球7.5万台电脑的“僵尸”病毒，还有让80万台电脑受到感染的“隐身猫”病毒。

2010年2月8日，金山云安全监测中心宣布紧急病毒预警，称“极虎”木马下

载器已经完全爆发，仅2月7日一天，就有100390台计算机感染该病毒。短时间内被袭击的用户计算机超过50万台，并导致大部分安全软件失效。嚣张的病毒团伙在虎年给网民定制了一份病毒“巨无霸”套餐，威力比“熊猫烧香”强数倍。

据安全部门透露，在利益的驱使下，病毒的制作、传播和销售已经越来越产业化，如果不提高普通用户的网络安全意识，未来几年中病毒将给我们造成不可估量的损失。

1.2 五花八门的网络威胁

互联网发展到今天，上网冲浪渐渐变成一种时尚，越来越多的人选择网上交友、网上购物、网上炒股、网络游戏……网络有利可图，不法分子和别有居心的人也就趁机而入，这使得普通网民在享受网络生活带来的便利的同时，也无时无刻不在面临着网络带来的威胁，稍有不慎就会中招，如图1-7所示。

图1-7 毫无防范的网民

1.2.1 被窃取和破坏的个人数据

每个人都有一些不想让别人知道的秘密，也就是隐私，但现在网络上却时不时出现个人隐私泄露，甚至有些企业机密、国家机密也难逃被窃取的厄运，由此造成的潜在威胁更是耸人听闻。我们平时常用的QQ空间、开心网和博客等，如果设置的账户密码过于简单，或者安全问题的答案易于破解，就容易被别有用心的人加以利用，导致个人信息流失。如果是网银账户和股票交易账户密码失窃，更是会直接造成用户的重大经济损失，后果不堪设想。有的人为便于记忆，喜欢将密码设置成生日或是电话号码，这其实是相当危险的，在这里奉劝各位谨慎设置密码，否则损失不可估计。

人们常说的“木马”病毒就是以盗取用户账户信息为目的的。其实只要设置安全级别较高的密码，并做好木马查杀工作，一般就能够比较有效地应对这种威胁。但还有一类病毒不是盗取信息，而是直接将信息损毁。如前面提到的PolyBoot引导区病毒，可以将整个硬盘格式化，这对用户来说可谓是“灭顶之灾”。

1.2.2 钓鱼网站的骗术

当你收到一封来自银行或者某电子商务网站的邮件，写着“恭喜中奖”、“领取奖金”或者“温馨提醒”等一系列主题时，这时一定要小心了。这很可能是钓鱼网站放出来的诱饵。如果你点击邮件的链接进入了这些网站，一般会被询问个

人信息，如果善良的你不加防备，可能就要成为上钩的“鱼”了，如图1-8所示。

图1-8　网络钓鱼诱惑不小

提示：所谓“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码，以此来骗取用户银行或信用卡账号、密码等私人资料。由此可以看出，除了来自计算机病毒的威胁，一些网络形式的骗术也会给网民造成很大的损失。如果说计算机病毒是来自程序的威胁，那么钓鱼网站的攻击更多是来自人的威胁。

1.2.3　僵尸网络

僵尸网络（见图1-9）是攻击者通过传播僵尸程序，感染并控制大量主机而形成的一个攻击平台，而这些被控制的主机就被形象地称为“僵尸”，众多的普通网民就在不知不觉中帮助一些攻击者进行着恶意的攻击行为。僵尸网络对当今的网络安全构成重大威胁，它是以点扩散到面的危害，攻击者利用手中一个攻击平台，可以攻击到整个基础信息网络甚至使系统瘫痪，个人的隐私信息和企业的商业秘密都会因此而泄露。

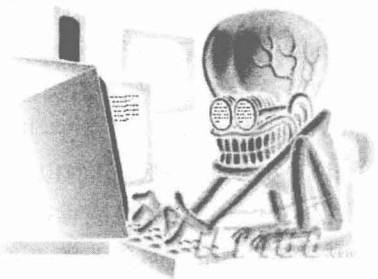


图1-9　僵尸网络带来的损失无法估计

美国互联网软件安全公司NetWitness在2010年爆出惊人消息，一种新型电脑病毒已入侵全球2500家企业和政府机构的7.5万台电脑，病毒将这些电脑构成了一个庞大而危险的“僵尸网络”，从中窃取重要资料，包括雅虎、Hotmail以及Facebook等社交网络都对这种病毒束手无策。安全机构进一步指出，一般的反恶意软件和基于签名的入侵探测系统均无法有效检测与防堵这种“僵尸”病毒。

计算机安全专家认为，犯罪集团可能来自东欧，许多商业公司和政府机构都在此波攻击中遭受牵连。目前，在线银行、雅虎、Hotmail、Facebook以及政府计算机系统都是该病毒侵害的目标对象。

1.3 认清网络安全的元凶

上一节所提到的种种网络威胁，或多或少都是借助病毒程序来实施的。因此，要应对网络威胁，排除安全隐患，首先要认清其始作俑者——计算机病毒——的真正面目。

1.3.1 认识计算机病毒

计算机病毒的历史可以追溯到20世纪80年代。如果要给它下个定义的话，可以说它是**在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码**。归根结底，病毒是一种计算机程序。它的种种活动并不像很多人想象的那样神秘，只要加以了解就能够防御大多数的病毒程序。

病毒不是来源于突发或偶然的原因。一次突发的停电或偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。病毒则是一种比较完美的、精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应，相互配合完成一定的功能。现在流行的病毒是由人为故意编写的，多数病毒可以找到作者和产地信息。从大量的统计分析来看，病毒作者主要情况和目的是：一些天才的程序员为了表现自己和证明自己的能力，出于对上司的不满，或因为好奇、报复、祝贺和求爱，或为了得到控制口令，或为了防止软件拿不到报酬预留的陷阱等。当然也有因经济、政治、军事、宗教、民族和专利等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。

计算机病毒一般都具有以下几个特点：

- 寄生性：计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发现的。
- 传染性：计算机病毒不但本身具有破坏性，更严重的是具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。
- 潜伏性：有些病毒像定时炸弹一样，它什么时间发作是预先设计好的。
- 隐蔽性：计算机病毒具有很强的隐蔽性，有的可以通过防病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。
- 破坏性：计算机中毒后，可能会导致正常的程序无法运行，计算机内的文件被删除或受到不同程度的损坏，通常表现为：增、删、改、移。

- 可触发性：因某个事件或数值的出现，诱使计算机病毒实施感染或进行攻击的特性称为可触发性。

1.3.2　常见计算机病毒分类

在了解病毒的起源和基本概念后，下面对病毒的主要分类做一个简要的介绍。

1. 引导区病毒

引导区病毒隐藏在硬盘或软盘的引导区，当计算机从感染了引导区病毒的硬盘或软盘启动，或从受感染的硬盘或软盘中读取数据时，引导区病毒就开始发作。一旦它们将自己复制到机器的内存中，马上就会感染其他磁盘的引导区，或通过网络传播到其他计算机上。

2. 文件型病毒

文件型病毒寄生在其他文件中，常常通过对它们的编码加密或使用其他技术来隐藏自己。文件型病毒劫夺用来启动主程序的可执行命令，用作它自身的运行命令。同时还经常将控制权还给主程序，伪装程序正常运行。一旦运行被感染了病毒的程序文件，病毒便被激发，执行大量的操作，并进行自我复制。

3. 脚本病毒

脚本病毒依赖一种特殊的脚本语言（如VBScript、JavaScript等）起作用，同时需要软件或应用环境能够正确识别和翻译这种脚本语言中嵌套的命令。脚本病毒在某些方面与宏病毒类似，但脚本病毒可以在多个产品环境中进行，还能在其他所有可以识别和翻译它的产品中运行。脚本语言比宏语言更具有开放终端的趋势，这样使得病毒制造者对感染脚本病毒的机器可以有更多的控制力。

4. 网络蠕虫程序

网络蠕虫程序是一种通过间接方式复制自身的非感染型病毒。有些网络蠕虫利用E-mail向世界各地发送自己的复制品；有些则出现在高速下载站点中传播自身；有些则同时使用两种方法传播。它的传播速度相当惊人，成千上万的病毒感染造成众多邮件服务器先后崩溃，给人们带来难以弥补的损失。由于会发送大量的病毒邮件，该病毒往往会导致网络变慢甚至瘫痪。

5. “特洛伊木马”程序

特洛伊木马程序通常是指伪装成合法软件的非感染型病毒，但它不进行自我复制。有些木马可以模仿运行环境，收集所需的信息。最常见的木马便是试图窃取用户名和密码的登录窗口，或者试图从众多的Internet服务器提供商(ISP)盗窃用户的注册信息和账号信息，如图1-10所示。